Data Security

Lecture No. (4)

Dr/ Roayat Ismail

Modern Cryptography

Modern symmetric-key ciphers

Since traditional ciphers are no longer secure, modern symmetric-key ciphers have been developed during the last few decades. Modern ciphers normally use a combination of substitution, transposition and some other complex transformations to create a ciphertext from a plaintext.

Modern ciphers are bit-oriented (instead of character-oriented).

The plaintext, ciphertext and the key are strings of bits.

Figure 30.9 *XOR cipher*

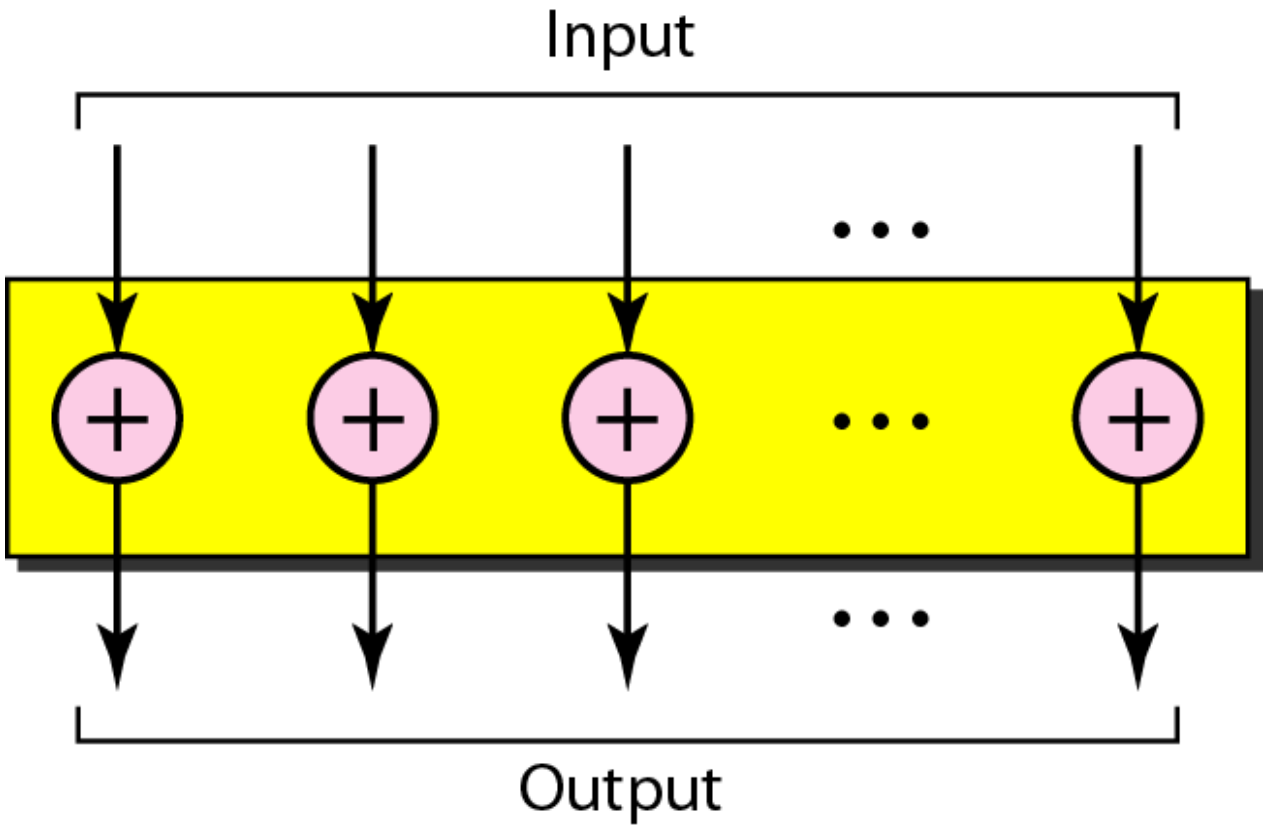


Figure 30.10 *Rotation cipher*

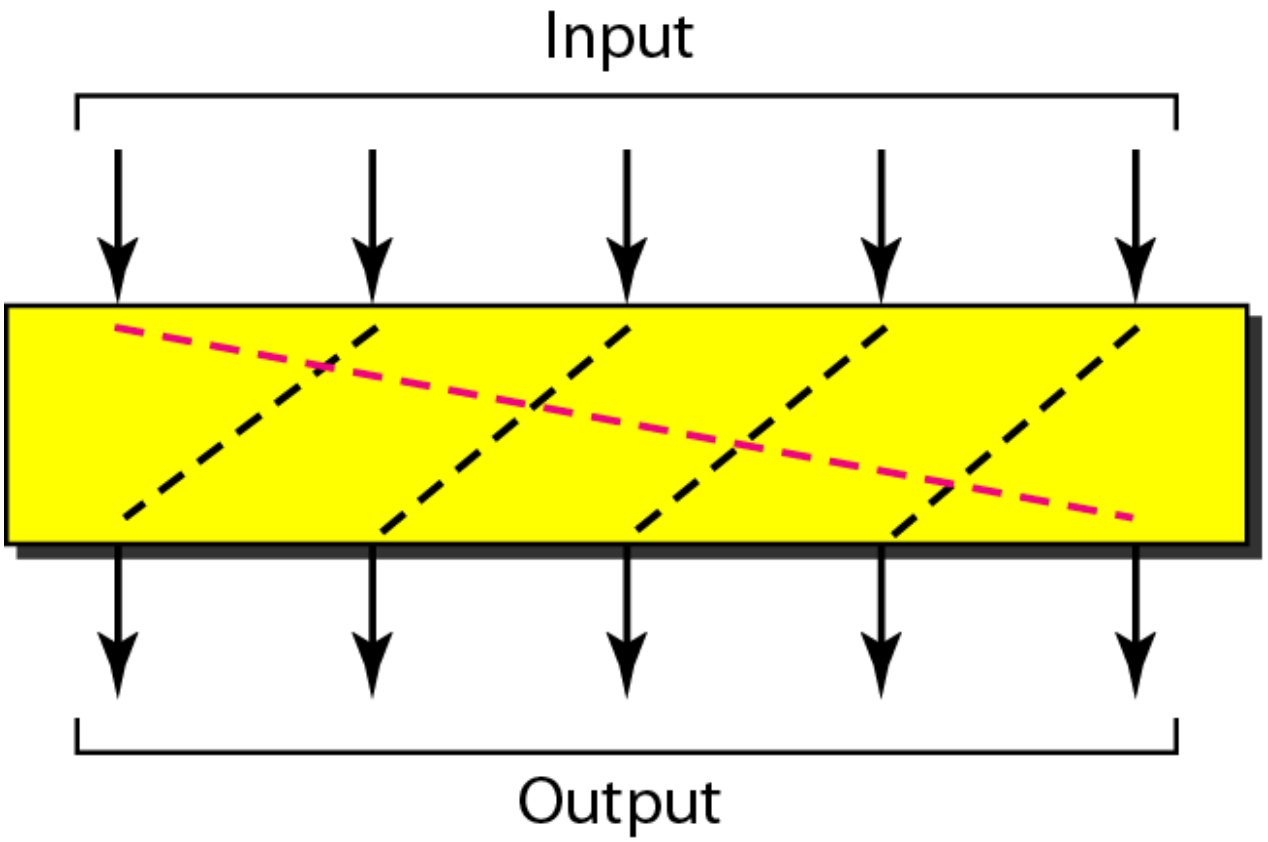


Figure 30.11 *S-box (substitution box)*

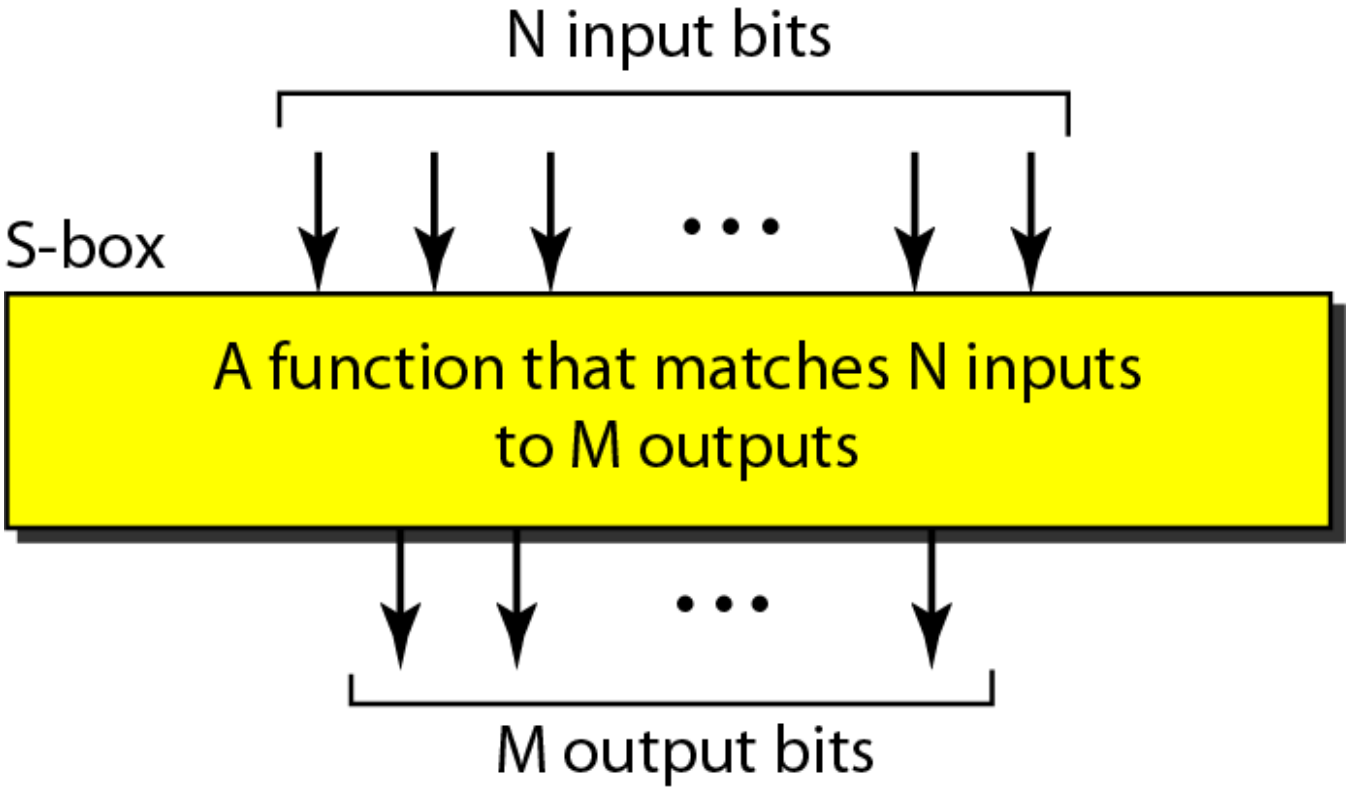
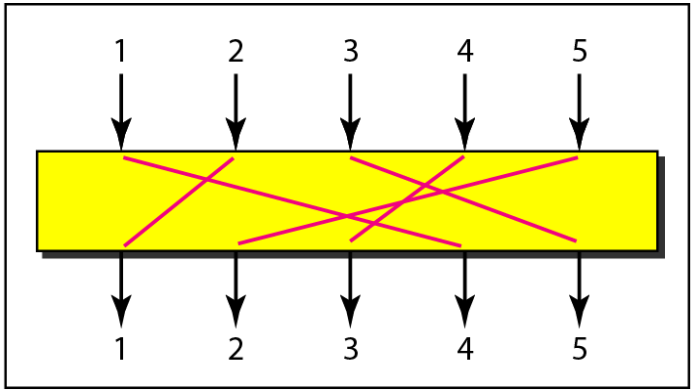
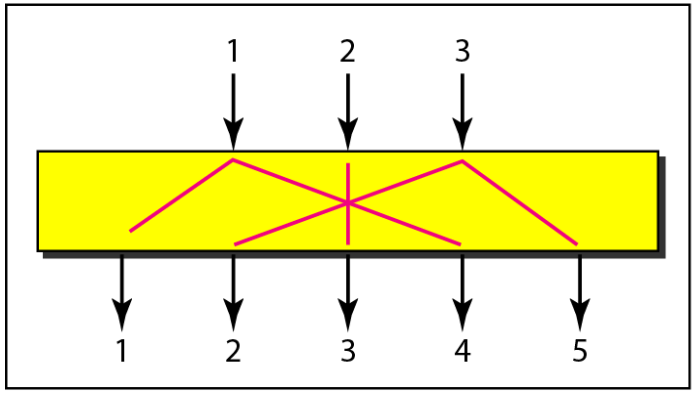


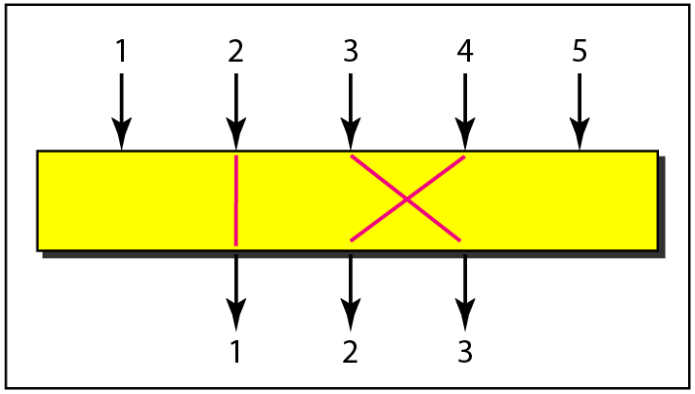
Figure 30.12 *P-boxes (permutation box): straight, expansion, and compression*



a. Straight



b. Expansion

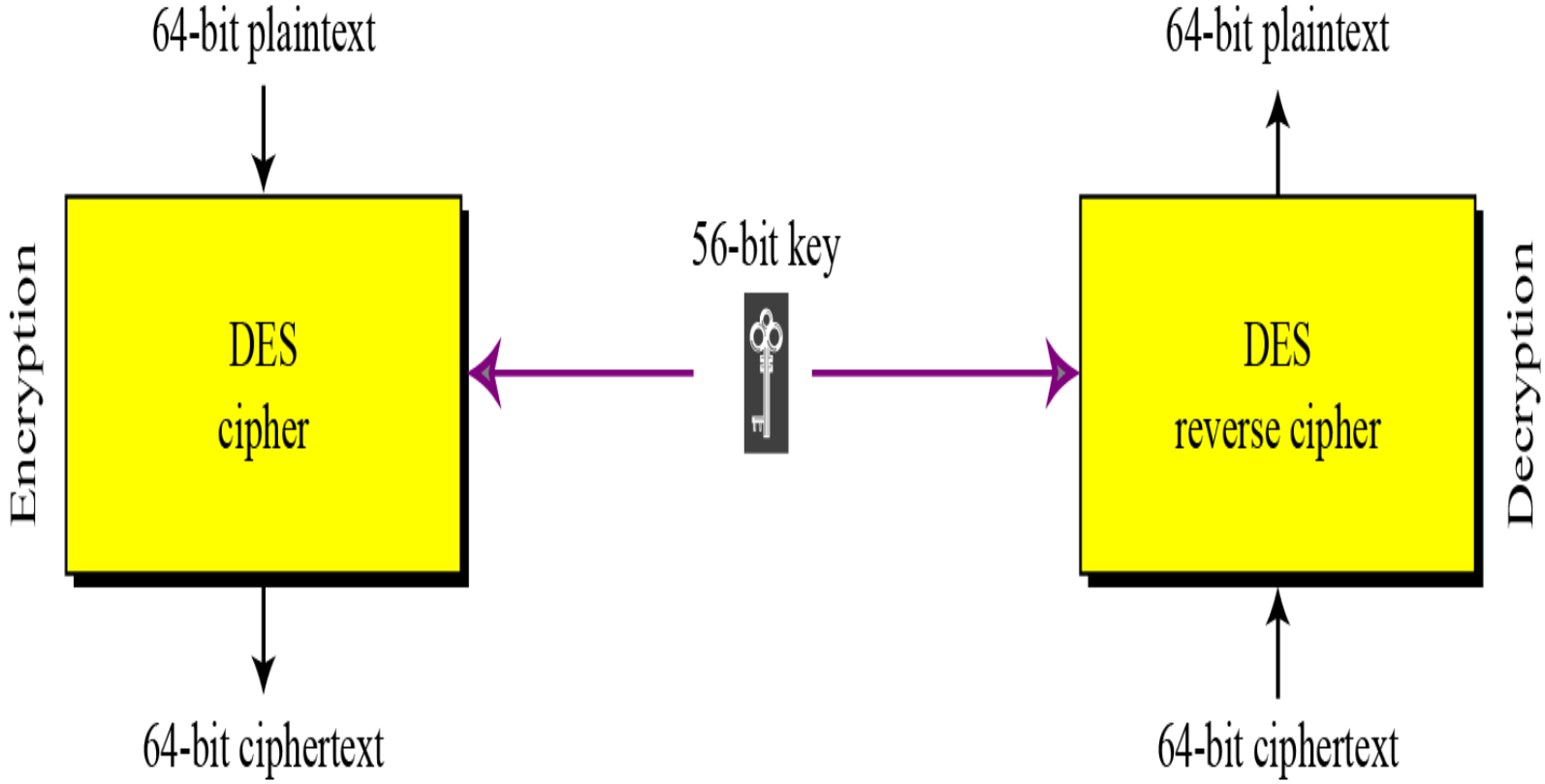


c. Compression

1. DES (Data Encryption Standard)

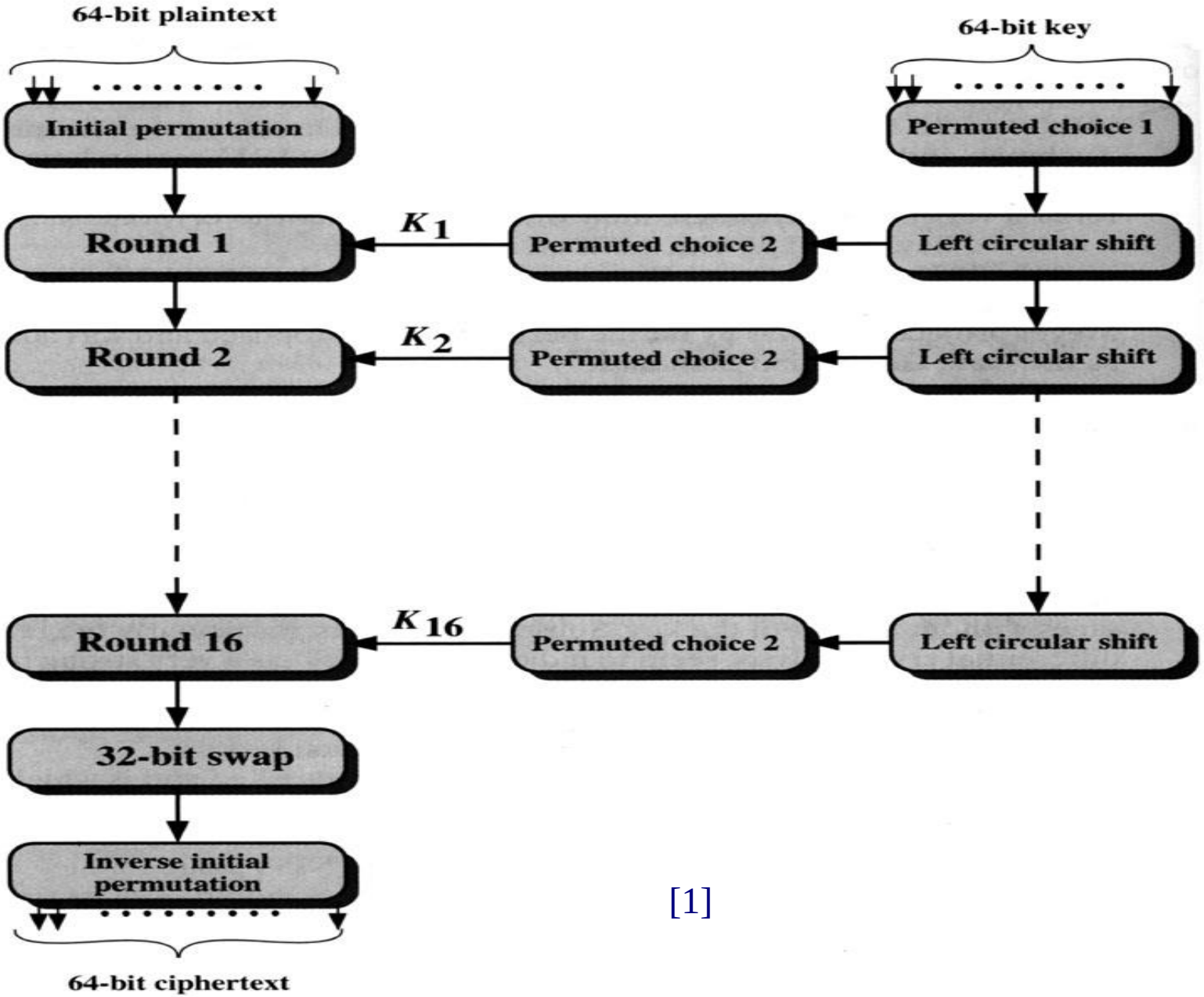
DES is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in 1977. DES has been the most widely used symmetric-key block cipher since its publication .

- Five ingredients,
  - Plaintext
  - Secret Key
  - Encryption algorithm
  - Ciphertext
  - decryption algorithm
- All operations of encryption and decryption are based on two basic kinds of manipulations on the data.
  - Permutation (transposition)
  - Substitution



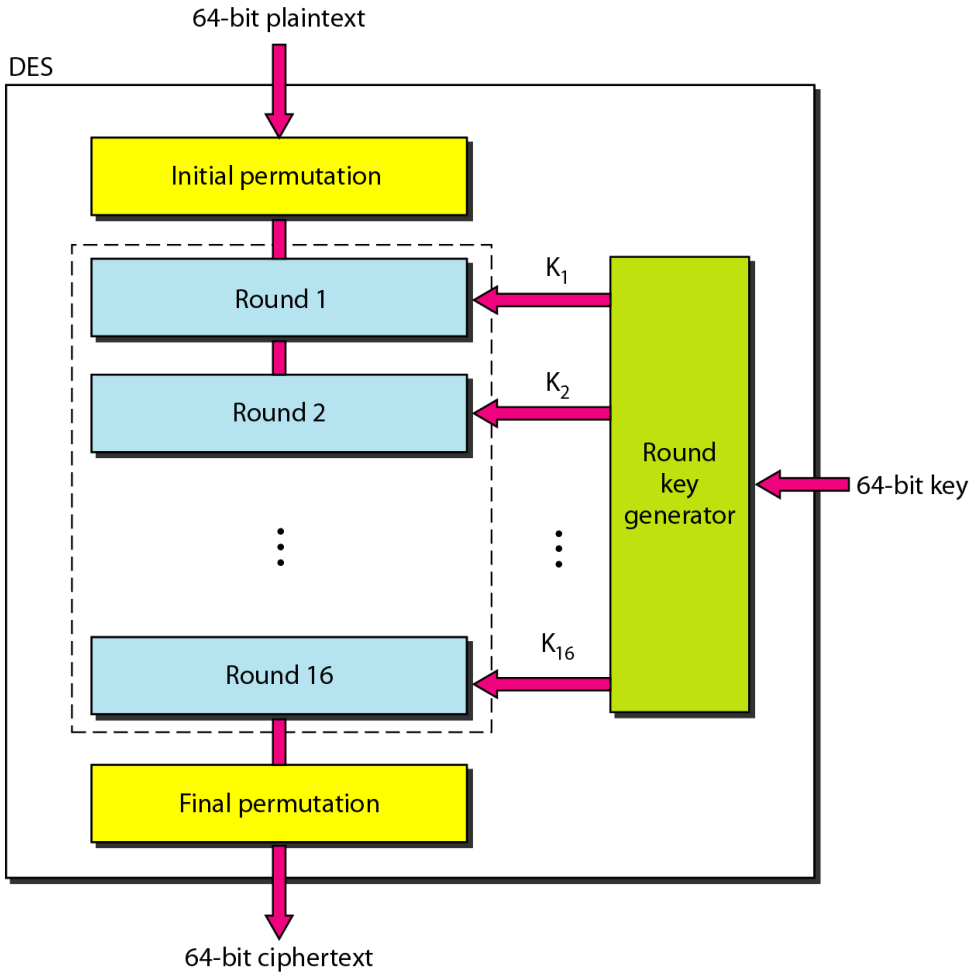
The general design of the DES encryption cipher

Encryption



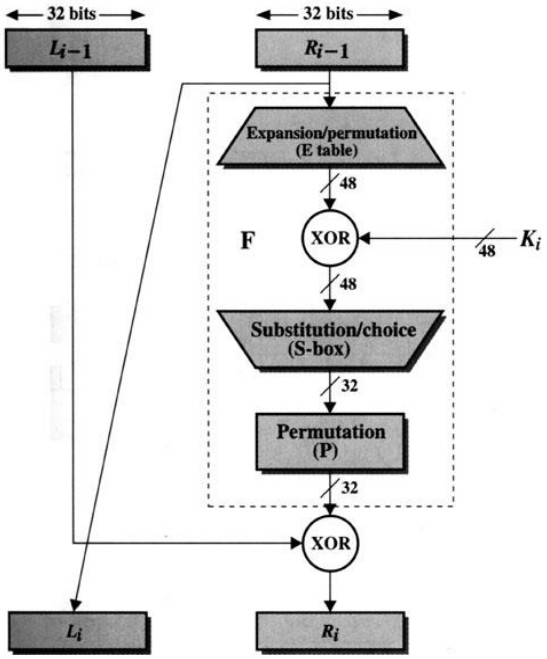
[1]

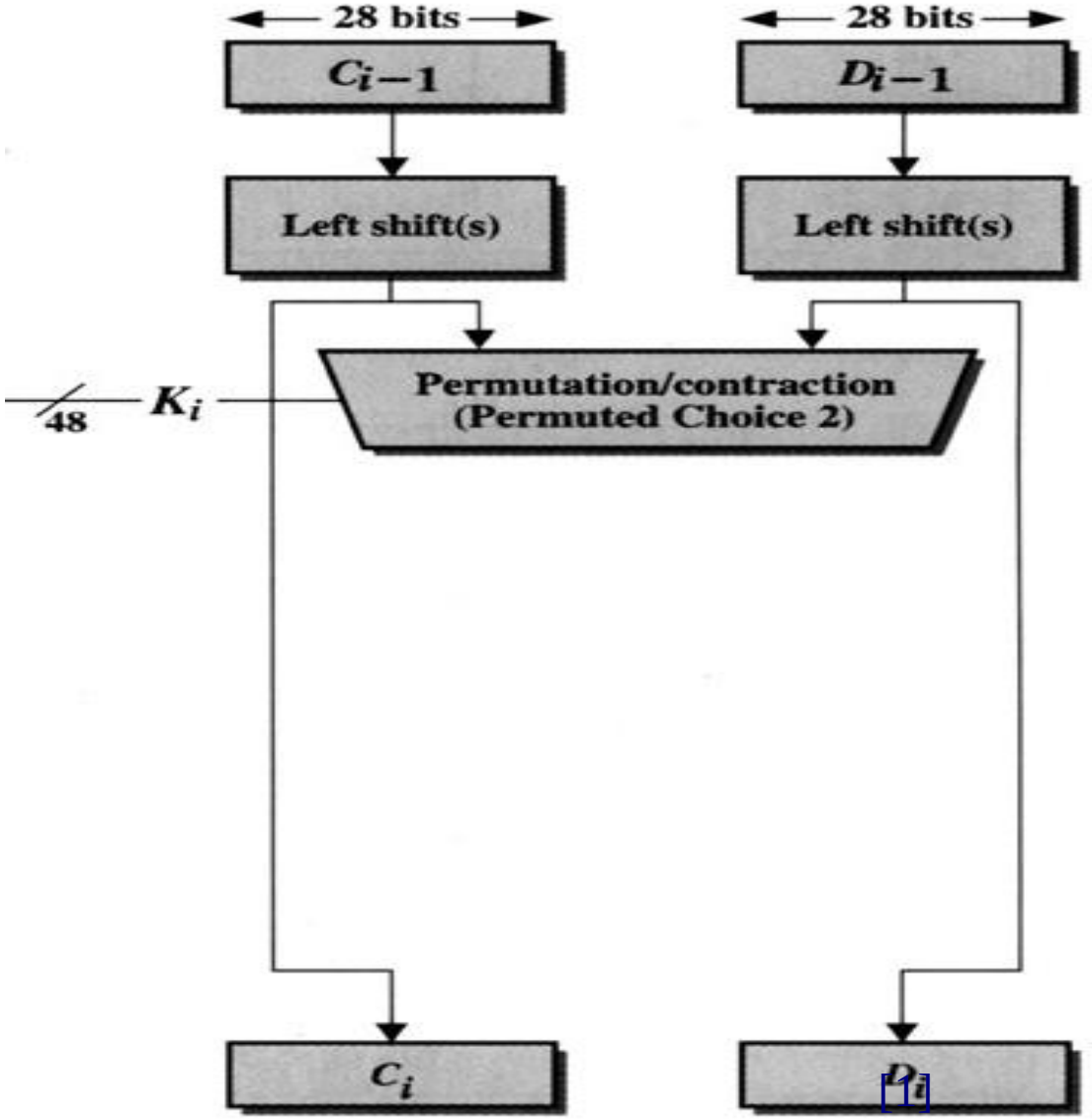
Figure 30.13 *DES (Data Encryption Standard)*



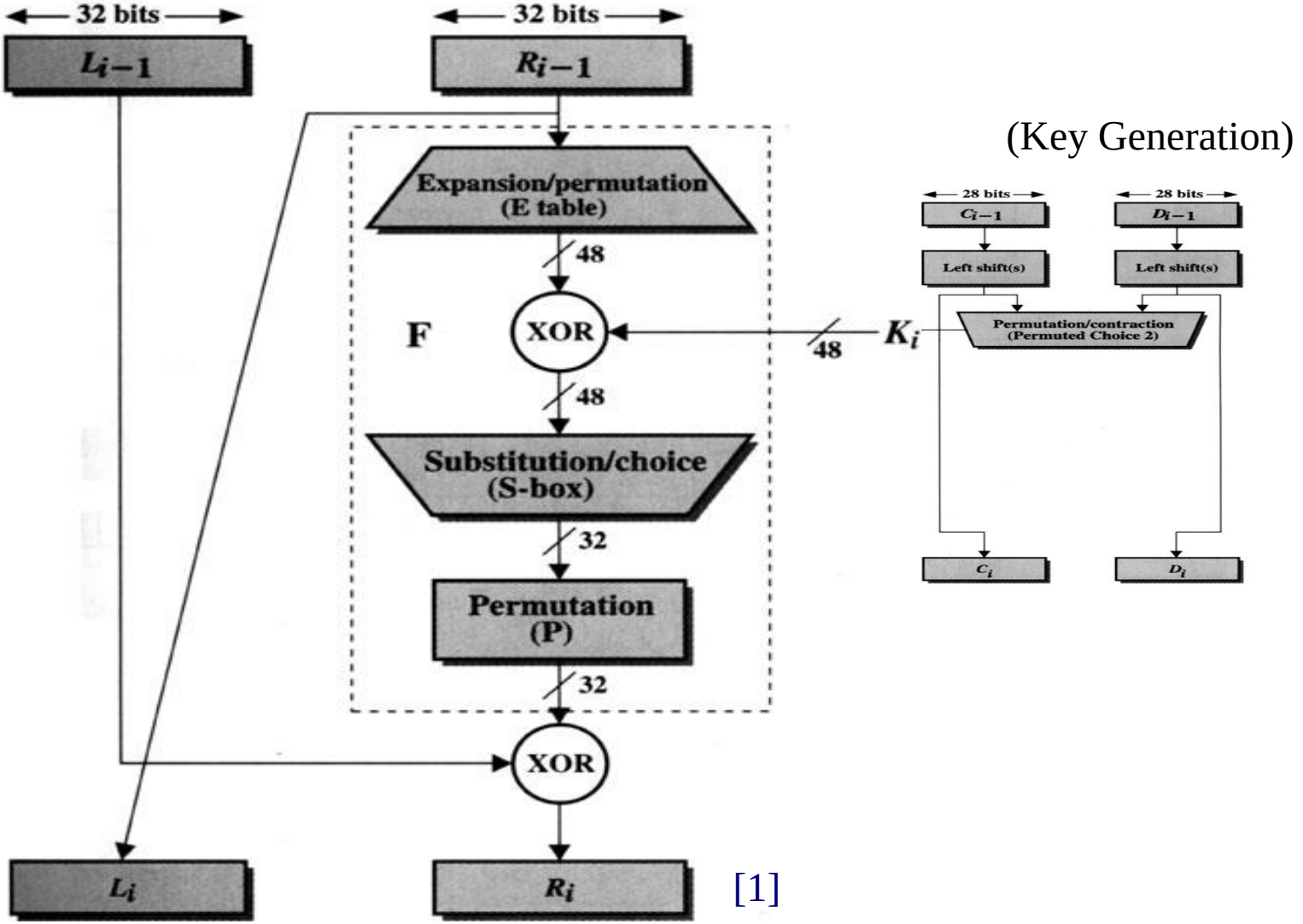
Key Generation

(Encryption)



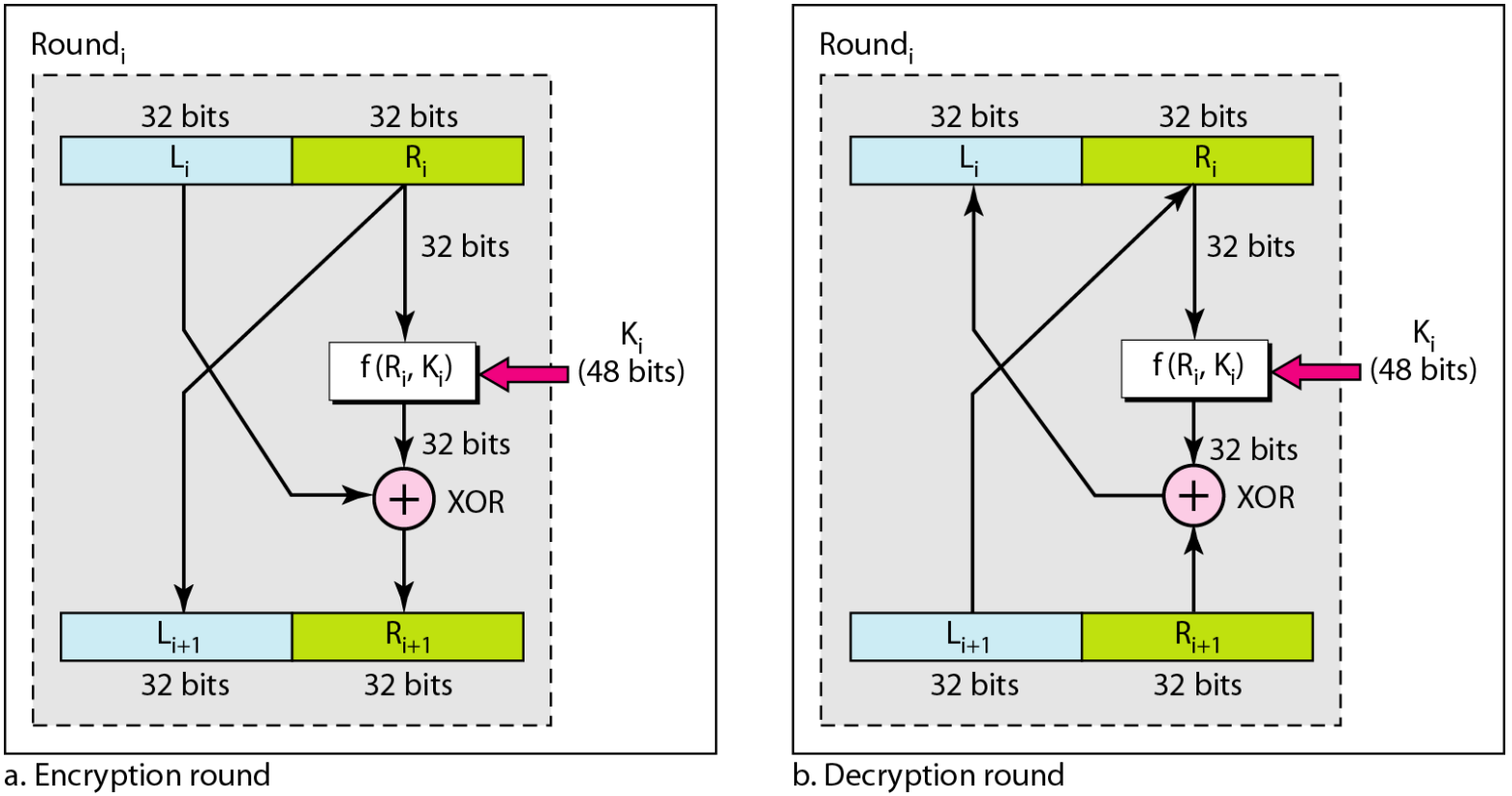


Encryption (Round)



[1]

Figure 30.14 *One round in DES ciphers*



The Strength/Weakness of DES

- Number of possible keys = 2^{56}
- Which is equivalent to 7.2 X 10^{16}
- On Average half the key space has to be searched
- Estimated single machine brute-force search

Key serch machine cost	Expected search time
$100,000	35 hours
$1,000,000	3.5 hours
$10,000,000	21 minutes

Parallel computing and improvement in computing power makes DES breakable.

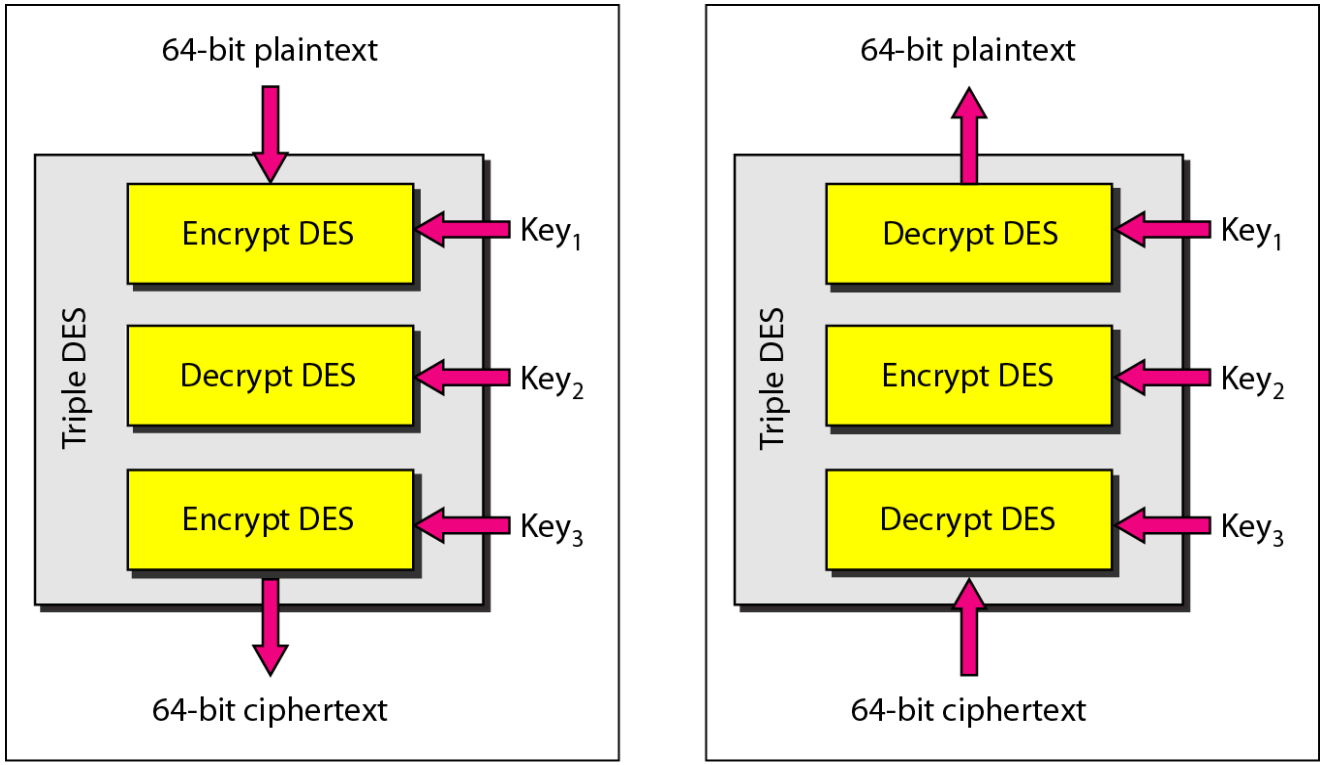
DES: Comments

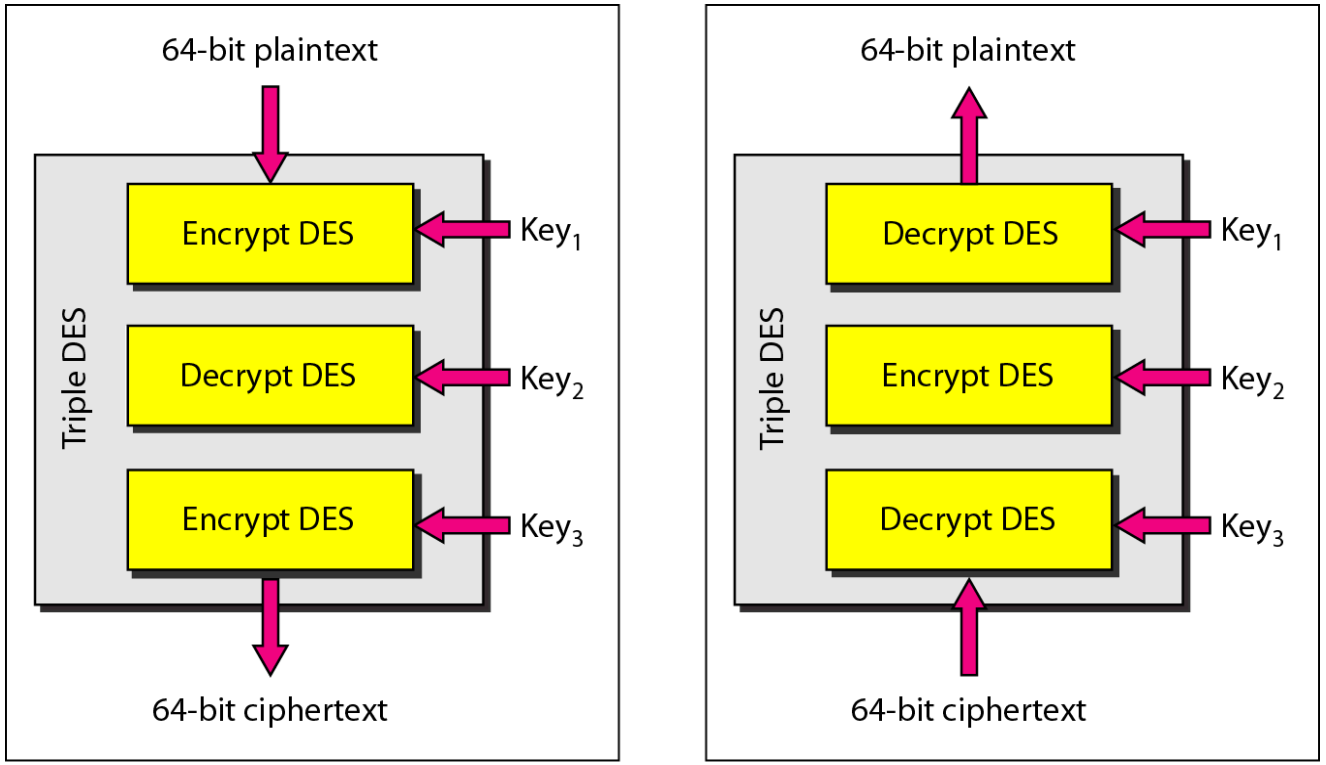
- 56 bit keys have become easier to break by exhaustive search (try all possible keys).

To solve this problem DES is replaced with:

- Modified DES (e.g., triple DES) protocols are used.
- DES will be replaced Advanced Encryption System (AES).

Figure 30.16 *Triple DES (to resolve the short key issue for DES)*





a. Encryption Triple DES

b. Decryption Triple DES

AES (Advanced Encryption System)

- As DES is getting very old, NIST began a public process to choose a new cipher to be called AES (Advanced Encryption Standard).

- AES algorithms should have 3 key sizes: 128, 192, 256 bits, and operate on block sizes of 128 bits.

AES is a symmetric-key block cipher published by the US National Institute of Standards and Technology (NIST) in 2001 in response to the shortcoming of DES, for example its small key size.

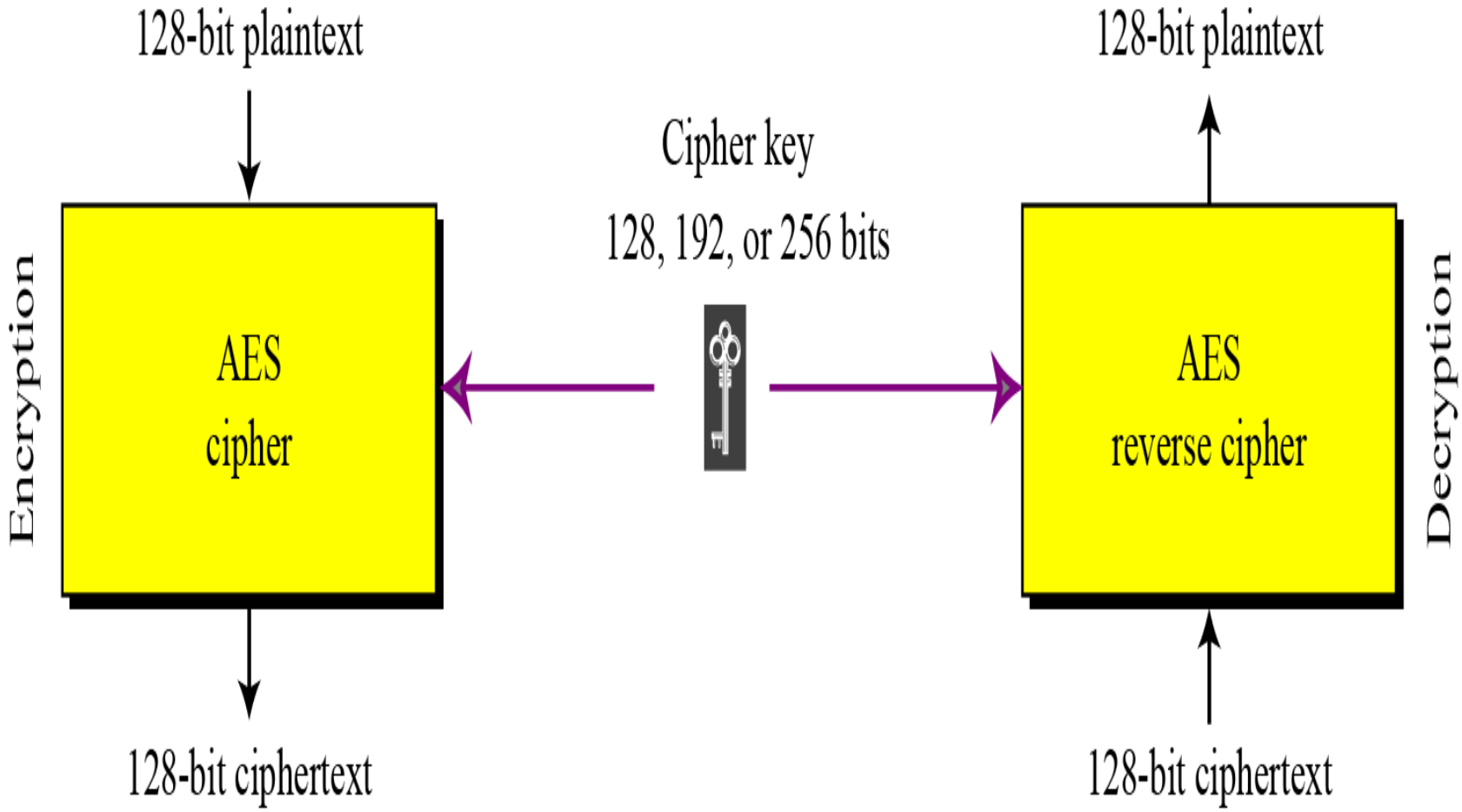
Table 30.1 *AES (advanced encryption standard) configuration*

Size of Data Block	*Number of Rounds*	*Key Size*
128 bits	10	128 bits
	12	192 bits
	14	256 bits

AES is the replacement of DES

Note

AES has three different configurations with respect to the number of rounds and key size.



Encryption and decryption with AES

Advantages of symmetric-key encryption

- Fast encryption and decryption algorithms.

- Larger key values make it harder to guess the key value -- and break the code -- by brute force.

Disadvantages of symmetric-key encryption

1. Requires secure transmission of key value
2. Requires a large number of keys (for n users it requires n (n-1)/2)

   For example, to have a separate key for each pair of 100 user would need 4950 different keys.